4. RECOMENDAÇÕES

Neste capítulo, estão elencadas as recomendações técnicas elaboradas pela equipe técnica profissional e capacitada, com o objetivo de orientar a execução de tarefas, processos ou a tomada de decisões. Essas recomendações são fundamentadas em conhecimentos técnicos, pesquisas e experiências práticas, visando garantir a eficiência, do programa de adequação da organização.

Recomendações

As recomendações técnicas apresentadas neste Relatório de Impacto à Proteção de Dados (RIPD) são fundamentadas em uma análise detalhada dos processos e práticas de tratamento de dados pessoais. O objetivo é fornecer diretrizes claras e ações específicas que visam mitigar riscos, fortalecer a conformidade com a Lei Geral de Proteção de Dados (LGPD), e assegurar a proteção dos dados pessoais de forma eficaz e contínua.

Baseado nas estatísticas apresentadas pelo sistema, o consultor indicou os seguintes pareceres técnicos:

Importante | Armazenamento | Computador Colaboradores

Importante | Contrato | Alunos - Cláusula 3.8 - Consentimento

Importante | Segurança da Informação

Importante | Cláusulas contratuais | Operadores

Importante | Descarte/Eliminação de dados

Importante | Políticas e Planos

Importante | Nomeação DPO e Comitê

Importante | Reconhecimento Facial | Catracas

Recomendável | Utilização WhatsApp

Recomendável | Informatizar atendimento aos titulares de dados

A seguir, serão detalhados as recomendações técnicas, divididas por áreas estratégicas, oferecendo uma visão abrangente e prática para orientar a empresa na adoção de melhorias contínuas em suas operações de tratamento de dados pessoais.

Armazenamento | Computador Colaboradores

Importante

Área de Preocupação:
Segurança de Informações

Ponto de atenção:

Conforme identificado durante o mapeamento, a instituição de ensino não possui procedimentos ou diretrizes formalizados para o armazenamento de documentos e dados pessoais nos computadores utilizados pelos colaboradores. Dessa forma, os arquivos são armazenados de maneira descentralizada e de acordo com as práticas individuais de cada usuário, sem critérios institucionais definidos quanto à localização, acesso, retenção e eliminação das informações.

O armazenamento descentralizado aumenta os riscos de acesso não

autorizado, perda ou extravio de informações, cópias não controladas, dificuldade de rastreabilidade, retenção de dados por períodos superiores ao necessário e impossibilidade de garantir a eliminação adequada dos dados pessoais.

Recomendação:

Recomenda-se a formalização de uma política ou procedimento de armazenamento de informações, estabelecendo os ambientes autorizados, níveis de acesso, regras de retenção e eliminação, bem como a priorização de ambientes corporativos centralizados e controlados. O armazenamento local deverá ser restrito a situações em que haja necessidade operacional, mediante aplicação de controles de segurança adequados, como controle de acesso, proteção por senha, backup e eliminação após o cumprimento da finalidade. Recomenda-se também a realização de verificações periódicas e orientação dos colaboradores quanto às regras estabelecidas.

Responsáveis pela implementação: o TI deverá apoiar a definição dos ambientes, controles de acesso e mecanismos de backup. As áreas responsáveis pelos processos deverão definir as necessidades de armazenamento e respectivos prazos de retenção. O DPO/Encarregado, quando aplicável, deverá orientar quanto aos requisitos de proteção de dados e acompanhar a implementação das medidas.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos
- Dano reputacional

Autor: Jenifer Tainara da Silva Cardoso em 06/10/2026 19:01

Contrato | Alunos - Cláusula 3.8 - Consentimento

Importante

Área de Preocupação:

Áreas e Processos

Ponto de atenção:

Analisando o contrato enviado, percebeu-se que a Cláusula 3.8 do contrato de prestação de serviços educacionais estabelece autorização prévia e abrangente para a utilização da imagem, nome e aproveitamento escolar do aluno, mediante diferentes formas de divulgação, incluindo fotografias, vídeos, materiais impressos, televisão, mídias digitais, redes sociais, outdoors, concursos, campeonatos escolares e outras modalidades de divulgação, inclusive para fins de divulgação e propaganda da instituição.

Recomendação:

A Cláusula 3.8, na redação atualmente adotada, apresenta abrangência excessiva e baixo nível de especificidade e transparência quanto às diferentes formas de utilização da imagem, nome e informações escolares dos alunos. Recomenda-se sua revisão e a adoção de instrumento específico para autorizações facultativas de uso de imagem e voz, com especial atenção aos tratamentos que envolvam crianças e adolescentes.

Ademais, orienta-se a leitura do parecer técnico sobre a cláusula.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 08/10/2026 16:27

Importante

Área de Preocupação:
Segurança de Informações

Ponto de atenção:

(1) Considerando a inexistência de documento formal que explicite a política de segurança da informação.

(2) Considerando a ausência de documentos e informações complementares, quanto a atenção para com a segurança da informação.

(3) Considerando a inexistencia de nomeação formal de um gestor de segurança da informação.

Recomenda-se:

Recomendação:

(1) Desenvolver e formalizar documentalmente o Programa de Segurança da Informação, estabelecendo suas diretrizes, objetivos, controles e procedimentos aplicáveis à instituição.

(2) Designar formalmente um responsável pela gestão da Segurança da Informação, definindo suas atribuições, funções e responsabilidades, bem como sua atuação na implementação, no acompanhamento e na melhoria dos controles de segurança.

As recomendações específicas referentes aos controles de Segurança da Informação avaliados pela consultoria estão disponíveis nos formulários correspondentes, acessíveis na caixa “Segurança da Informação” do organograma.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 30/10/2026 17:08

Cláusulas contratuais | Operadores

Importante

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

Considerando a análise dos fornecedores, incluindo a avaliação dos contratos disponibilizados, recomenda-se a adoção das seguintes medidas para fortalecimento da conformidade e mitigação de riscos relacionados à proteção de dados pessoais:

Recomendação:

Para os **operadores classificados como de risco crítico ou grave**, recomenda-se a adoção de medidas formais e reforçadas de conformidade com a LGPD:

1. Solicitação de Documentação e Declarações de Conformidade

Deve-se **formalizar o envio de solicitações** aos operadores, requerendo:

- Documentos comprobatórios de suas práticas de segurança da informação;
- Declarações de aderência à LGPD e às diretrizes internas da instituição;

- Indicação de um **encarregado (DPO)** e dos canais de contato para assuntos de privacidade.

Essas providências visam assegurar que os operadores adotam medidas adequadas de proteção de dados e compreendem suas responsabilidades legais.

2. Revisão e Inclusão de Cláusulas Contratuais Específicas

É **obrigatória a inclusão de cláusulas de responsabilidade e proteção de dados pessoais** nos contratos vigentes e nos que vierem a ser celebrados com operadores. Essas cláusulas devem especificar:

- As obrigações de segurança e confidencialidade;
- A limitações de uso dos dados pessoais;
- Os procedimentos para comunicação de incidentes de segurança;
- As penalidades em caso de descumprimento;
- As regras para exclusão ou devolução dos dados ao término do contrato.

Recomenda-se, ainda, revisar os contratos atuais, substituindo cláusulas genéricas por disposições mais detalhadas e alinhadas à realidade operacional de cada serviço.

3. Atenção à Análise Contratual

Observou-se que, em diversos casos, as disposições contratuais sobre proteção de dados são **genéricas e insuficientes**, não delimitando claramente as responsabilidades das partes, local de armazenamento, as medidas de segurança adotadas e os fluxos de tratamento das informações.

Essa fragilidade pode gerar riscos de responsabilização solidária e comprometer a conformidade institucional.

4. Armazenamento e Transferência de Dados

Outro ponto crítico identificado é a **falta de clareza sobre o armazenamento dos dados pessoais**. Deve-se exigir dos operadores informações detalhadas sobre:

- O local de armazenamento dos dados (ambiente próprio, servidor terceirizado ou nuvem);
- A identificação do responsável direto pelo armazenamento;
- A existência de transferência internacional de dados, incluindo o país de destino e os mecanismos de proteção utilizados (como cláusulas contratuais padrão ou certificações).

Essas informações são essenciais para garantir transparência, segurança e aderência às exigências legais previstas na LGPD.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 30/10/2026 17:09

Descarte/Eliminação de dados

Importante

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

(1) Considerando a inexistência de documentação relacionado a retenção e descarte dos dados pessoais.

(2) Considerando a ausência de processo de retenção e descarte de documentos lógicos e físicos.

Recomenda-se

Recomendação:

(1) Elaborar e validar a norma de retenção e descarte pré-desenvolvido

pela consultoria.

(2) Operacionalizar e gerar evidência formal quanto aos processos de retenção e descarte de dados pessoais.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 30/10/2026 17:16

Políticas e Planos

Importante

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

(1) Considerando a inexistência de políticas e planos formalizados voltados à proteção de dados pessoais e à segurança da informação, bem como a necessidade de adequá-los à realidade atual da instituição e à legislação vigente;

(2) Considerando os riscos decorrentes do descumprimento das exigências legais e da ausência de adoção de boas práticas relacionadas à proteção de dados pessoais;

Recomenda-se:

Recomendação:

(1) Que a Escola Bilíngue Harmonia aprove e implemente formalmente as políticas e os documentos desenvolvidos pela consultoria,

promovendo sua divulgação interna e a capacitação periódica dos colaboradores, a fim de assegurar o conhecimento e o cumprimento das diretrizes estabelecidas.

(2) Que as políticas classificadas como públicas sejam disponibilizadas nos canais oficiais de comunicação da instituição, de modo a garantir transparência e facilitar o acesso às informações pelos titulares de dados pessoais e demais interessados.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 30/10/2026 17:21

Nomeação DPO e Comitê

Importante

Área de Preocupação:
Governança

Ponto de atenção:

(1) Considerando a necessidade de formalizar a indicação de um Encarregado pelo Tratamento de Dados Pessoais (DPO), responsável por atuar como canal de comunicação entre a instituição, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD), bem como orientar os colaboradores e apoiar a instituição no cumprimento da LGPD;

(2) Considerando a importância de estabelecer uma estrutura de governança em privacidade e proteção de dados, com participação de representantes das áreas estratégicas e operacionais da instituição;

(3) Considerando a necessidade de promover a integração entre os setores, acompanhar a implementação das medidas de adequação à

LGPD e apoiar a gestão dos riscos relacionados ao tratamento de dados pessoais;

Recomenda-se:

Recomendação:

Formalizar a nomeação do Encarregado pelo Tratamento de Dados Pessoais (DPO), com definição de suas atribuições, responsabilidades e canais de contato, bem como instituir um Comitê de Privacidade e Proteção de Dados, composto por representantes das áreas pertinentes da instituição, com responsabilidades relacionadas ao acompanhamento das ações de conformidade, à avaliação de riscos, à análise de incidentes e ao fortalecimento da cultura de proteção de dados pessoais.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 30/10/2026 17:28

Reconhecimento Facial | Catracas

Importante

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

(1) Considerando que determinadas unidades da Escola Bilíngue Harmonia utilizam tecnologia de reconhecimento facial para controle de acesso de alunos e colaboradores;

(2) Considerando que essa tecnologia envolve o tratamento de dados

biométricos, classificados como dados pessoais sensíveis pela LGPD, inclusive de crianças e adolescentes;

(3) Considerando a necessidade de avaliar a conformidade desse tratamento com a legislação aplicável, especialmente quanto à hipótese legal, à necessidade e à proporcionalidade da utilização da biometria, bem como à proteção dos direitos dos titulares;

Recomenda-se:

Recomendação:

Submeter a utilização do sistema de reconhecimento facial a uma avaliação técnica e jurídica especializada, a fim de verificar sua adequação à LGPD e às normas de proteção de crianças e adolescentes, incluindo o ECA Digital, quando aplicável, especialmente quanto à hipótese legal que fundamenta o tratamento, à eventual necessidade de consentimento dos titulares ou responsáveis legais e à existência de alternativas para o controle de acesso.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 30/10/2026 17:36

Utilização WhatsApp

Recomendável

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

Conforme informações obtidas nas entrevistas, foi identificada a utilização de contas particulares de WhatsApp para comunicação institucional e recebimento de documentos, sem a definição de diretrizes ou procedimentos padronizados pela instituição para o tratamento e armazenamento das informações compartilhadas.

Recomendação:

Desse modo, recomenda-se estabelecer diretrizes para utilização do WhatsApp nas comunicações institucionais, priorizando o uso de contas corporativas e restringindo o tratamento de dados pessoais por contas particulares. Também devem ser definidos procedimentos para o recebimento, armazenamento e eliminação de documentos e informações compartilhados pelo aplicativo.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos
- Dano reputacional

Autor: Jenifer Tainara da Silva Cardoso em 06/10/2026 10:40

 Informatizar atendimento aos titulares de dados Recomendável

Área de Preocupação:

Áreas e Processos

Ponto de atenção:

(1) Considerando a necessidade de disponibilizar e divulgar um canal de comunicação específico para que os titulares de dados pessoais possam exercer seus direitos e encaminhar solicitações à instituição;

(2) Considerando a necessidade de estabelecer procedimentos para o recebimento, gerenciamento, acompanhamento e resposta às

requisições dos titulares de dados pessoais;

(3) Considerando a importância de manter registros e evidências documentais das solicitações recebidas, das providências adotadas e das respostas fornecidas, de modo a demonstrar o atendimento aos direitos dos titulares, nos termos da LGPD;

Recomenda-se:

Recomendação:

Utilizar a aplicação PRIVIA (Módulo de Requisições), disponibilizada no escopo dos serviços contratados, para registrar, gerenciar e acompanhar as solicitações dos titulares de dados pessoais, permitindo documentar as etapas de atendimento e manter evidências das providências adotadas pela instituição.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 30/10/2026 17:25